Application Number 09/900,493
Responsive to Advisory Action mailed October 27, 2006

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Claim 1 (Currently Amended): A method for enabling secure communication between a client on an open network and a server apparatus on a secure network, the method performed on an intermediary apparatus coupled to the secure network and the open network, comprising:

negotiating, with the intermediary apparatus, a secure communications session with the client ~~apparatus~~ via the open network, wherein the secure communications session provides for communication of application data from the client to the intermediary apparatus via a plurality of security records, and wherein one or more of the security records includes encrypted application data spanning multiple data packets;

negotiating, with the intermediary apparatus, an open communications session with the server via the secure network;

receiving, with the intermediary apparatus, one or more of the data packets for a first one of the security records using the secure communications session ~~encrypted packet application data for a security record spanning multiple data packets, wherein the security record has a length greater than a packet length associated with the multiple data packets~~;

prior to receiving a final packet of the first one of the security records, processing the one or more data packets of the first one of the security records with the intermediary apparatus by decrypting the encrypted ~~packet~~ application data in ~~each~~ the received data packets,[[;]] forwarding decrypted, unauthenticated application data from the intermediary apparatus to the server via the secure network prior to authenticating the first one of the security records with the intermediary apparatus,[[;]] and discarding at least a portion of the decrypted, unauthenticated ~~packet~~ application data for the first one of the security records ~~prior to receiving a final packet of the security record~~; and

upon receipt of the final packet of the first one of the security records, processing a remaining, non-discarded portion of the decrypted, unauthenticated application data for the first one of the security records to authenticate ~~authenticating~~ the first one of the security records with the intermediary apparatus ~~on receipt of the final packet of the security record~~.

Claim 2 (Previously Presented): The method of claim 1 wherein forwarding includes: forwarding data which spans over multiple TCP segments.

Claim 3 (Cancelled).

Claim 4 (Currently Amended): The method of claim 1 wherein ~~only~~ the a remaining, non-discarded portion of the ~~packet~~ application data for the first one of the security records is buffered by the intermediary apparatus as a minimal length sufficient to complete a block cipher used to encrypt the data.

Claim 5 (Currently Amended): The method of claim 1 wherein authenticating includes authenticating the decrypted data for the first one of the security records upon receiving a final TCP segment of a multi-segment encrypted data stream and after forwarding the decrypted, unauthenticated application data received prior to the final TCP segment.

Claim 6 (Currently Amended): The method of claim 1 further including, after forwarding the decrypted, unauthenticated application data to the server, notifying the client ~~apparatus~~ if a failure in authenticating the first one of the security records occurs.

Claim 7 (Currently Amended): A method for processing encrypted data transferred between a first system and a second system, comprising:

providing an accelerator device including a decryption engine in communication with the first system via an open network and the second system via a secure network;

receiving encrypted application data from the first system via the open network in the form of security records communicated through a secure communications session, wherein one or more of the security records span ~~application data spanning~~ multiple packets, and wherein a last packet of the multiple packets in each of the security records includes information for authenticating the application data contained within that security record;

as the multiple packets are received for any of the plurality of security records, processing the multiple packets for that security record by:

(i) decrypting, with the accelerator device, the application data contained within the multiple packets ~~as the multiple packets are received~~;

(ii) forwarding the decrypted application data ~~as the multiple packets are decrypted~~ from the accelerator device to the second system ~~device~~ via the secure network as the multiple packets of the security record are decrypted by the accelerator device;

(iii) buffering, with the accelerator device, a first portion of the decrypted application data for the security record and discarding a ~~remaining~~ second portion prior to authentication of the application data of the security record; and

(iv) after discarding the second portion of the decrypted application data for the security record and upon receiving the information for authenticating the application data in the last of the multiple packets for the security record, authenticating the buffered, first portion of the application data of the security record ~~when the information for authenticating the application data is received in the last of the multiple packets~~.

Claim 8 (Previously Presented): The method of claim 7 wherein receiving comprises receiving SSL encrypted data.

Claim 9 (Previously Presented): The method of claim 7 wherein decrypting comprises decrypting application data encrypted using SSL and a DES algorithm.

Claims 10-11 (Cancelled)

Claim 12 (Previously Presented): The method of claim 7 wherein buffering comprises buffering the application data for a minimal length less than a security record but sufficient to complete a block cipher used to encrypt the data.

Claim 13 (Original): The method of claim 12 wherein said block cipher is a form of DES.

Claim 14 (Currently Amended): The method of claim 7 wherein authenticating includes alerting the first system ~~device~~ if authenticating fails after forwarding the decrypted, unauthenticated application data that is received prior to the last one of the multiple packets.

Claim 15 (Currently Amended): The method of claim 7 wherein authenticating includes generating a reset to the second system ~~device~~ if said authenticating fails.

Claim 16 (Currently Amended): A method of providing secure communications using limited buffer memory in an ~~processing~~ intermediary device, the secure communications providing a plurality of secure socket layer (SSL) records over an SSL session, the method comprising:

receiving, with the intermediary device, encrypted data for a portion of an SSL record, wherein the SSL record has ~~having~~ a length greater than a TCP segment carrying said data;

buffering the encrypted data of the received portion of the SSL record in a memory buffer in the intermediary device, the buffer having a length equivalent to a block cipher size necessary to perform the cipher;

decrypting, with the intermediary device, the buffered ~~segment of the received~~ portion of the encrypted data to provide decrypted application data; and

forwarding the decrypted application data from the intermediary device to a destination device prior to authenticating the SSL record with the intermediary device.

Claim 17 (Original): The method of claim 16 wherein the block cipher is 3DES.

Claim 18 (Original): The method of claim 16 wherein the block cipher is DES.

Claim 19 (Currently Amended): The method of claim 16 further including authenticating the data with the intermediary device on receipt of a final segment of the encrypted data by the intermediary device after forwarding the unauthenticated application data of the SSL security record ~~that is received prior to the final segment~~.

Claim 20 (Previously Presented): The method of claim 19 further including generating an alert if authenticating results in a failure.